UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/881,145	06/14/2001	Craig Partridge	BBNT-P01-368	8070

28120 7590 11/30/2006

FISH & NEAVE IP GROUP
ROPES & GRAY LLP
ONE INTERNATIONAL PLACE
BOSTON, MA 02110-2624

EXAMINER	
DIVECHA, KAMAL B	

ART UNIT	PAPER NUMBER
2151	

DATE MAILED: 11/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/881,145	PARTRIDGE ET AL.	
	Examiner	Art Unit	
	KAMAL B. DIVECHA	2151	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 November 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,13-20,23 and 24* is/are pending in the application.

4a) Of the above claim(s) *11,12,21,22 and 25* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10, 13-20, 23, 24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Arguments

Claims 1-10, 13-20 are pending in this application.

Claims 23-24 have been cancelled in this application.

Applicant's arguments filed November 06, 2006, with respect to the above claims, have been fully considered but they are not persuasive.

a. Neither Conklin or Wong teach or suggest using a flag stored in memory to determine whether a target packet has been encountered (remarks, page 9, page 10).

In response to argument [a], Examiner respectfully disagrees in light of the following reasons:

Claim 1 stands rejected as follows:

As per claim 1, Conklin discloses in a network carrying a plurality of packets over at least one network link, said network including a computer, a first network component having memory and a processor and configured to store information in said memory about at least one of said plurality of packets, and a second network component (fig. 16), a method for detecting target packet comprising (col. 1 L10-65): receiving said at least one of said plurality of packets over a link to obtain a received packet (fig. 7, fig. 8, col. 3 L60-65); receiving a query message identifying a target packet at said first component (fig. 7, fig. 8, col. 3 L1-14); creating a reply if said target packet has been encountered (col. 4 L9-60, col. 5 L10-60, fig. 6, fig. 9); and said first network component making said reply available to said network if said target packet has been encountered, wherein reply is capable of being used as part of a method for locating said intrusion point for said first one of the packets (fig. 9),

However, Conklin does not disclose the process of determining a hash value of at least a portion of said packet; using said has value to identify a location in a memory; setting a flag in said memory, said flag associated with said location; and said first network component using a flag in processing said query message to determine if said target packet has been encountered (note that Conklin teaches the process of detecting an intrusion by pattern matching or comparing, see col. 7 L50-65, fig. 7).

Wong, from the same field of endeavor explicitly discloses the process of determining a hash value of at least a portion of said packet (fig. 2B item #222, fig. 2C item #242 and fig. 3C, fig. 6 item #602, col. 6 L4-8); using said hash value to identify a location in a memory (fig. 2B item #224, fig. 2C item #244, fig. 6 item #604); setting a flag in said memory, said flag associated with said location (fig. 6 item #608, fig. 8 item #818820, 822, col. 6 L4-15, col. 7 L28-36, col. 9 L6-33); and said first network component using a flag in processing said query message (a message or a packet) to determine if said target packet has been encountered (fig. 8 item #818, 820, 822 and fig. 6 item #608, 610, col. 5 L59-63, col. 6 L4-36).

Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Conklin in view of Wong in order to use the hashing technique to determine or identify the packet.

One of ordinary skilled in the art would have been motivated because it would have located and/or identified the packet (whether target, incoming or outgoing) in a more efficient manner, which would have reduced the latency in the network appliance (Wong, col. 2 L19-41, col. 3 L27-30, L45-51).

Wong explicitly teaches the process of using a flag stored in memory to determine if the target packet has been encountered, i.e. received.

Wong clearly teaches the process of using flag set in the memory for the purpose of indicating whether the packet is an inbound, i.e. incoming or received (note that in the claims the target packet is an incoming packet) or outbound, i.e. outgoing packet (see col. 6 L38-46).

Furthermore, Wong states "A has table entry that points to inbound/outbound flag, which is set, corresponds to an inbound packet. The set flag indicates that the packet that generated the match with the hash table is an inbound packet, i.e. an incoming packet or received packet (col. 7 L3-16).

Furthermore, Wong states "...The match looked for in the hash table depends on whether the pointer in the hash table points to an inbound/outbound flag that is set. If the inbound/outbound flag is set...if the inbound/outbound flag is set, then it is determined that the packet is an inbound packet, i.e. an incoming or received packet (col. 8 L10-33, col. 8 L60 to col. 9 L5).

As such Wong does teach the process of using the flag set in the memory to determine whether a packet, i.e. a target packet, has been received or encountered.

Therefore it would have been obvious to a person of ordinary skilled in the art to modify Conklin in view of Wong as set forth above.

Hence, applicant's argument directed towards using the flag to determine whether a packet has been received, is not persuasive.

b. Conklin and Wong fail to teach or suggest "...the hash of the packet is over the entire packet" (remarks, page 11, the subject matter as in claim 5).

In response to argument [b], Examiner disagrees.

Claim 5 stands rejected as follows:

As per claim 5, Conklin does not disclose the process wherein hash value is determined over the entire packet.

Wong, from the same field of endeavor discloses the process wherein the addresses in a packet are hashed (col. 5 L60 to col. 6 L35, fig. 2, fig. 5 and fig. 7-8: hashing technique).

Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Conklin in view of Wong in order to determine the hash value over the entire packet.

One of ordinary skilled in the art would have been motivated because of the same reasons as set forth in claim 1.

First, note that the claim does not teach the process wherein the entire packet is hashed, it simply suggests the hash value is determined "over" the entire packet, i.e. a portion of the packet being hashed can be interpreted as hashing over the entire packet.

In an event where the claim did suggest the process of determining a hash value of the entire packet or hashing the entire packet, Wong teaches the hashing technique of at least a portion of the packet (col. 5 L60 to col. 6 L35, fig. 2, fig. 5 and fig. 7-8: hashing technique).

If Wong's system is able to hash at least a portion of the packet, then Wong's system is capable of determining the hash value over the entire packet.

Therefore, it would have been obvious to a person of ordinary skilled in the art to modify Conklin in view of Wong in order to determine the hash value over the entire packet, simply because Wong teaches the process of determining a hash value for at least a portion of the packet.

Therefore, for the reasons set forth above, applicant's argument directed towards the distinction between the prior art and the claim limitation as in claim 5, is not persuasive.

c. The rejections of Independent claims 10 and 13 are improper (remarks, page 11).

In response to argument [c], Examiner respectfully disagrees because claims 10 and 13 do not teach or further define over the limitations of claim 1, as shown below.

For example: claim 13 is simply a system claim of the subject matter claimed in claim 1, i.e. a method claim.

Claim 1 recites:

In a network carrying a plurality of packets over at least one network link, said network including a computer, a first network component having memory and a processor and configured to store information in said memory about at least one of said plurality of packets, and a second network component, a method for detecting target packet comprising:

receiving said at least one of said plurality of packets over said link to obtain a received packet;

determining a hash value of at least a portion of said packet;

using said hash value to identify a location in said memory;

setting a flag in said memory, said flag associated with said location;

receiving a query message identifying a target packet at said first network component;

said first network component using said flag in processing said query message to determine if said target packet has been encountered:

creating a reply if said target packet has been encountered; and

said first network component making said reply available to said network if said target packet has been encountered.

Claim 10 recites:

In a network carrying a plurality of packets over at least one link, said network including a network component operatively coupled to said link and having a memory and a processor, a method for storing information about a plurality of packets received over said network, at least a portion of said information being used to locate an intrusion point for a first one of said plurality of packets, said method comprising:

receiving said first one of said plurality of packets;

determining a first hash value of said first one of said plurality of packets over at least a portion thereof;

usi ng said first hash value to identify a first location in said memory

setting a flag at said first location said flag indicating said first hash value has occurred;

receiving a second one of said plurality of packets;

processing said second one of said plurality of packets to obtain information contained therein;

using said information contained in said second one of said plurality of packets to determine if said first one of said plurality of packets has been observed; and

making a reply available to said network if said information contained in said second one of said plurality of packets indicates that said first one of said plurality of packets has been observed, said reply capable of being used as part of a method for locating said intrusion point for said first one of said plurality of packets.

Examiner would like to point out that rephrasing the terms such as "query message" to "second one of the plurality of packets" and "at least one of the plurality of packets" or "target packet" to "one of said plurality of packets" in the claims, do not change the scope of the claims.

The limitation "said first network component using said flag in processing said query message to determine if said target packet has been encountered" is equivalent to the process of "using said information contained in said second one of said plurality of packets (i.e. processing a query message) to determine of said first one said plurality of packets has been observed" (i.e. a target packet has been observed).

Applicant is further requested to differentiate the independent claims if the independent claims 1, 10 and 13 are different.

Furthermore, first and second interfaces, a bus and a memory are the core components of any computer system.

Therefore, The rejection of claims 10 and 13 is proper at least based on the claimed subject matter.

d. Neither Conklin nor Wong teaches or suggests processing a second packet to obtain information to determine whether a first packet has been observed (remarks, page 12).

In response to argument [d], Examiner disagrees.

Conklin teaches the process of receiving the plurality of packets, wherein the packets are of type ftp, www, telnet, etc. (page 3 L1-21).

Conklin is capable of receiving a message or a packet in a form of a www or telnet request, to determine if the network surveillance system has received any malicious attack or any

intrusion and reporting any detected intrusion in form of a reply or a report (see fig. 7, 8 and fig. 9).

Therefore, applicant's argument towards the distinction between the prior art and the claimed limitation as in [d] above is not persuasive.

DETAILED ACTION

Claim Rejections - 35 USC § 112

The rejection presented in the prior office action has been withdrawn due to cancellation of the claims 23-24.

Claim Rejections - 35 USC § 101

The rejection presented in the prior office action has been withdrawn due to cancellation of the claims 23-24.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

1. Claims 1-5, 7, 9, 10, 13-15, 17, 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Conklin et al. (hereinafter Conklin, U. S. Patent No. 5,991,881) in view of Wong et al. (hereinafter Wong, U. S. Patent No. 6,389,419 B1).

As per claim 1, Conklin discloses in a network carrying a plurality of packets over at least one network link, said network including a computer, a first network component having memory and a processor and configured to store information in said memory about at least one of said plurality of packets to locate an intrusion point, and a second network component (fig. 16), a method for detecting target packet comprising (col. 1 L10-65): receiving said at least one of said plurality of packets over a link to obtain a received packet (fig. 7, fig. 8, col. 3 L60-65); receiving a query message identifying a target packet at said first component (fig. 7, fig. 8, col. 3

L1-14); creating a reply if said target packet has been encountered (col. 4 L9-60, col. 5 L10-60, fig. 6, fig. 9); and said first network component making said reply available to said network if said target packet has been encountered, wherein reply is capable of being used as part of a method for locating said intrusion point for said first one of the packets (fig. 9),

However, Conklin does not disclose the process of determining a hash value of at least a portion of said packet; using said has value to identify a location in a memory; setting a flag in said memory, said flag associated with said location; and said first network component using a flag in processing said query message to determine if said target packet has been encountered (note that Conklin teaches the process of detecting an intrusion by pattern matching or comparing, see col. 7 L50-65, fig. 7).

Wong, from the same field of endeavor explicitly discloses the process of determining a hash value of at least a portion of said packet (fig. 2B item #222, fig. 2C item #242 and fig. 3C, fig. 6 item #602, col. 6 L4-8); using said hash value to identify a location in a memory (fig. 2B item #224, fig. 2C item #244, fig. 6 item #604); setting a flag in said memory, said flag associated with said location (fig. 6 item #608, fig. 8 item #818820, 822, col. 6 L4-15, col. 7 L28-36, col. 9 L6-33); and said first network component using a flag in processing said query message (a message or a packet) to determine if said target packet has been encountered (fig. 8 item #818, 820, 822 and fig. 6 item #608, 610, col. 5 L59-63, col. 6 L4-36).

Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Conklin in view of Wong in order to use the hashing technique to determine or identify the packet.

One of ordinary skilled in the art would have been motivated because it would have located and/or identified the packet (whether target, incoming or outgoing) in a more efficient manner, which would have reduced the latency in the network appliance (Wong, col. 2 L19-41, col. 3 L27-30, L45-51).

As per claim 2, Conklin discloses the process wherein making said reply available to said network includes forwarding said reply to said second network component (fig. 9, col. 5 L10-60).

As per claim 3, Conklin discloses the process wherein said second network component is a computer (fig. 9, col. 5 L10-60).

As per claim 4, Conklin discloses the process wherein said reply contains a network address for said first network component (col. 6 L9-15).

As per claim 5, Conklin does not disclose the process wherein hash value is determined over the entire packet.

Wong, from the same field of endeavor discloses the process wherein the addresses in a packet are hashed (col. 5 L60 to col. 6 L35, fig. 2, fig. 5 and fig. 7-8).

Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Conklin in view of Wong in order to determine the hash value over the entire packet.

One of ordinary skilled in the art would have been motivated because of the same reasons as set forth in claim 1.

As per claim 7, Conklin discloses the process wherein said network is an Internet Protocol (IP) network (fig. 1)

As per claim 9, Conklin discloses the process wherein said first network component is a router (fig. 1-3).

As per claim 14, Conklin discloses the system wherein said first interface and second interface are combined into a single bi-directional interface (fig. 4).

As per claim 15, Conklin discloses the process wherein said reply is made available to another network (fig. 9).

As per claim 19, the combination of Conklin and Wong discloses the system wherein said reply is positive reply if said second has value matches at least one of said plurality of first hash values.

As per claim 20, Conklin discloses the system wherein said reply is forwarded to those of said devices one hop away (fig. 9 and fig. 3).

As per claims 10, 13 and 17, they do not teach or further define over the limitations in claims 1-5, 7, 9, 14-15, 19 and 20. Therefore claims 10, 13 and 17 are rejected for the same reasons as set forth in claims 1-5, 7, 9, 14-15, 19 and 20.

2. Claims 8, 16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Conklin et al. (hereinafter Conklin, U. S. Patent No. 5,991,881) in view of Wong et al. (hereinafter Wong, U. S. Patent No. 6,389,419 B1), and further in view of "Official Notice".

As per claim 8, Conklin in view of Wong does not explicitly disclose the process wherein the link is a wireless link or network.

But, wireless networks and/or links are well known in the relevant art.

Official Notice is taken in order to indicate that the subject matter is in fact well known and obvious in the art.

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Conklin in view of Wong in order to implement the invention in wireless networks.

One of ordinary skilled in the art would have been motivated because wireless networks are very well known in the art.

As per claim 18, Conklin in view of Wong does not explicitly disclose a system wherein the processor is an ASIC processor.

But, ASIC processors are simply well known and obvious in the relevant art.

Official Notice is taken to indicate that the ASIC processors are known and obvious in the art.

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Conklin in view of Wong in order to include ASIC processors.

One of ordinary skilled in the art would have been motivated because ASIC processors are simply known in the art.

As per claim 16, it does not teach or further define over the limitations in claim 8 and 18. Therefore claim 16 is rejected for the same reasons as set forth in claim 8 and 18.

3. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Conklin et al. (hereinafter Conklin, U. S. Patent No. 5,991,881) in view of Wong et al. (hereinafter Wong, U. S. Patent No. 6,389,419 B1), and further Cox et al. (hereinafter Cox, U. S. Patent No. 6,842,861).

As per claim 6, Conklin in view of Wong does not teach the process of determining if said received packet has undergone a transformation, such transformation having occurred if a first hash value of at least a portion of said packet computed at a first time is not equal to a second hash value of at least a portion of said packet computed at a second time, said second time occurring after said first time.

Cox teaches determining if said received packet has undergone a transformation, such transformation having occurred if a first hash value of at least a portion of said packet computed at a first time is not equal to a second hash value of at least a portion of said packet computed at a second time, said second time occurring after said first time (col.2, L 34-41).

Therefore it would have been obvious to one ordinary skilled in the art at the time of the invention to modify the teaching of Wong to add determining if said received packet has undergone a transformation, such transformation having occurred if a first hash value of at least a portion of said packet computed at a first time is not equal to a second hash value of at least a portion of said packet computed at a second time, said second time occurring after said first time as taught by Cox in order to determine infected files (Cox, col. 2, line 34).

One ordinary skilled in the art at the time of the invention would have been motivated to combine Cox and Wong in order to provide a system to detect a file with a virus (Cox. col.1, lines 5-67).

Additional References

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Sheymov, U. S. Patent No. 6,981,146 B1: Network Intrusion Protection.

b. Vaidya, U. S. Patent No. 6,279,113 B1: Network Intrusion Detection.

Conclusion

Applicant's Invention is directed to a method and system comprising the process of receiving a malicious traffic at a network node; generating a query message in response to receiving the malicious packet; sending the query message to routers that are one hop away, which indeed will further transfer the query to routers that are one hop away to the first router, wherein the query message is for determining whether the routers has encountered the malicious packet, building the trace of the path to determine the malicious packet ingress point, and in response to determination, notifying the management system or intrusion detection system to disable the path (see fig. 4).

In order to expedite the prosecution in this application, applicant is advised to consider incorporating the subject matter in accordance with the figure 4 of the applicant and figure 5, into the independent claims, which would make the claimed invention distinct from the above rejection.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAMAL B. DIVECHA whose telephone number is 571-272-5863. The examiner can normally be reached on Increased Flex Work Schedule.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Zarni Maung can be reached on 571-272-3939. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kamal Divecha
Art Unit 2151
November 20, 2006.

WILLIAM VAUGHN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100